pmrt

29 March 2016

Instructions for Gaining Access to Project Management Resource Tools (PMRT)

General Information:

PMRT is accessed via https://pmrt.altess.army.mil/pmrt/

A Common Access Card (CAC) is required to access PMRT and to digitally sign the DD Form 2875.

PMRT is a suite of five tools. You can use a single 2875 form to gain access to all of them:

- Web CCaR
- Executive CCaR
- Data Access Program Reporting (DAPR)
- Enterprise Reports
- Resource Identification Tool (RIT)

Step 1: Decide which PMRT tool you need.

- For Access to Web CCaR you must specify the module privileges you are requesting. Using the drop-down menus, select the roles you need. Please specify the database and org you require access to in Block 13a. If you require access to multiple databases, please specify the database(s) and organization(s) you require access to as well as the associated roles in Block 27. For an explanation Web CCaR roles, see below.
- For Access to Executive CCaR, you must type in the program or org you want to have visibility at. If you require access to multiple program/org nodes please specify the additional nodes you require access to in Block 27.

  You do not need to select a role for a tool that you don't want to access—just leave it blank. There are no drop-downs For Executive CCaR; you must type in the program or org you want access to.
- For Access to DAPR you must specify the role you are requesting. Use the drop down menu to select the role that you are requesting. For an explanation of DAPR roles, see below.
- For access to Enterprise reports you need to specify the report folder that you are requesting access to. If you require access to multiple report folders, please specify this in Block 27.
- For access to the Resource Identification Tool you must specify the DAPR role that you are requesting. Use the drop-down menu to select the desired role. If multiple roles are required, please specify the additional roles you are requesting in Block 27.

Step 2: Follow instructions to complete 2875 listed below.

The completion of the digital signature is always the last step for each individual completing the form, prior to saving and sending it forward. This means that the following Blocks should be the last Blocks updated on the form:

Block 11 (when saved by the Requestor)
Block 18 (when saved by the Supervisor)
Block 31 (when saved by the Security Manager)
Block 22 (when saved by the Information Assurance Owner (IAO) also known as the Cybersec Liaison. Note: The Security Manager can also serve as the IAO
Block 21 (when saved by the Information Owner)

Step 2a: To be completed by the Requestor:

TYPE OF REQUEST: Indicate INITIAL by checking the box.
DATE: Type in today's date in YYYYMMDD format.
SYSTEM NAME: Type in "PMRT"
LOCATION: Type in "ALTESS"
Block 1: Type in the requestor's Full Name.
Block 2: Type in the requestor's Organization.
Block 3: Type in the requestor's Office Symbol or Department.
Block 4: Type in the requestor's complete Commercial Telephone Number.
Block 5: Type in the requestor's official work E-mail Address.
Block 6: Type in the requestor's Job Title and Grade/Rank.
Block 7: Type in the requestor's Official Mailing Address.
Block 8: Check the applicable box for the requestor's Citizenship.
Block 9: Check the applicable box for the requestor's Designation (check only one box).
Block 10: Check that you have completed the Annual Information Awareness Training check box and the date the training was completed.
Block 12: Leave blank (when electronically signed, the date signed will display in block 11).
Block 13: Utilize the drop downs and data entry fields to specify what PMRT tools you require access to and the corresponding module privileges and/or access level needed.
Block 13a: Type in the justification for access to the requested PMRT tools.
Block 14: Indicate AUTHORIZED by checking the box.
Block 15: Indicate UNCLASSIFIED by checking the box.
Block 16a: If the requestor is a CONTRACTOR this block needs to be completed with the Company Name, Contract Number, and Expiration Date. Additional contract information that may entered in Block 27, please refer back to Block 16a.
If the contract has EXPIRED, this form will be sent back to the Requestor.
Block 27: Utilize this field to specify additional information regarding your access request. Please see step 1a-1e above for examples of additional information that may be tracked in Block 27.
Block 11: This is the last step the requestor should complete prior to sending the form to their supervisor. The requestor must click the "sign here" flag and use a valid ID certificate from their CAC to sign the form. After signing, the form will prompt the user to Save. The requestor will save the file using the following naming convention:

LastNameFirstName_CCaRDB_CCaROrg_PMRTDD2875

Examples:
DoeJane_SMC_LE_PMRTDD2875
DoeJohn_FB_A10_PRMTDD2875
SmithJohn_MULTIPLE_MULTIPLE_PMRTDD2875

*Use "MULTIPLE in place of CCaRDB if requesting access to multiple CCaR databases
*Use "MULTIPLE" in place of CCaROrg if requesting access to multiple CCaR orgs in the requested database

NOTE: The requestor should now e-mail the form to their supervisor for approval.

Step 2b: To be completed by the Supervisor:

Block 13: Verify that the requestor is authorized to view the data access requested.
Block 16: Verify that the requestor has a Need To Know by checking the box.
Block 17: Type in the supervisor's Name.
Block 19: Leave blank (when electronically signed, the date signed will display in block 18).
Block 20: Type in the supervisor's Organization and Department.
Block 20a: Type in the supervisor's official work E-mail Address.
Block 20b: Type in the supervisor's complete Commercial Telephone Number.
Block 18: This is the last step the supervisor should perform prior to sending the form to the security manager. The supervisor must click the "sign here" flag and use a valid ID certificate from their CAC to sign the Form. After signing, the form will prompt the user to Save.

NOTE: The supervisor should now e-mail the form to the local security manager for security validation.

Step 2c: To be completed by the Security Manager:

Block 28: Type in the Type of Investigation.
Block 28a: Type in the Date of Investigation.
Block 28b: Type in the Clearance Level.
Block 28c: Type in the IT Level Designation.
Block 29: Type in the security manager's name.
Block 30: Type in the security manager's telephone number.
Block 32: Fill out today's date in YYYYMMDD format.
Block 31: This is the last step the Security Manager should perform prior to sending the form to the requestor. The Security Manager must click the "sign here" flag and use a valid ID certificate from their CAC to sign the Form. After signing, the form will prompt the user to Save.

NOTE: The security manager should now e-mail the form to the local IAO (also referred to as a Cybersec Liaison)

Step 2d: To be completed by the IAO:

Block 23: Type in the IAO Organization or Department.
Block 24: Type in the IAO phone number.
Block 25: Fill out today's date in YYYYMMDD format.
Block 22: This is the last step the IAO should perform prior to sending the form to the information owner. The security manager must click the "sign here" flag and use a valid ID certificate from their CAC to sign the Form. After signing, the form will prompt the user to Save.

NOTE: The IAO should now e-mail the form to Information Owner

Step 2e: To be completed by the Information Owner:

Block 21a: Type in the Information Owner's phone number.
Block 21b: Fill out today's date in YYYYMMDD format.
Block 21: This is the last step the Information Owner should perform prior to sending the form to the Help Desk for processing. The Information Owner must click the "sign here" flag and use a valid ID certificate from their CAC to sign the Form. After signing, the form will prompt the user to Save.

NOTE: The information Owner should now e-mail the form back to the requestor and store the completed 2875 locally. The PMRT Program office will coordinate with each Information Owner to upload the stored 2875's to a centralized repository.

Step 3: Route the approved 2875 to the appropriate destination(s)

1. To request PMRT access:
    - The requestor must navigate to https://pmrt.altess.army.mil/pmrt/; clicks Sign In; authorize themselves using their CAC; completes the PMRT online registration form; uploads the completed DD2875; and clicks Register.

2. To request Web CCaR access:
    - The requester must forward the completed 2875 to the CCaR administrator.
        i. The CCaR administrator will create the Web CCaR account, set the permissions based upon the approved 2875, and upload the 2875 into Web CCaR.

    NOTE 1: If requesting access to multiple Web CCaR databases, the 2875 needs to be forwarded to the CCaR administrator for each DB.

    NOTE 2: If requesting access to databases that are outside of the scope of the information owner, the user must also provide an email approval from the other information owner stating their approval to have access to the database.

3. To request Executive CCaR access:
    - The requester must forward the completed 2875 to the ALTESS Executive CCaR helpdesk (army.altess.servicedesk@mail.mil).

Explanation of PMRT Roles

Web CCaR

Web CCaR is part of the PMRT suite of tools. Access to Web CCaR can be through PMRT or through a direct link. Role based management within Web CCaR is primarily accomplished through the assignment of privileges to each of the modules that make up Web CCaR. Details on each of the modules and the privileges for each module are displayed below:

- **CCaR Module Privileges**
  - **None**: prevents the user from accessing the database.
  - **Read-Only**: allows the user read-only access to the Program Management (PM), Financial Management (FM) and Reports menus.
  - **User-OPR**: allows the user to only view CCaR records where they are assigned as an OPR or Back-up OPR. The user can create new CCaR records and edit existing CCaR records where they are assigned as the OPR. The user is prevented from accessing many reports and tools. Reports and tools accessible to the user will only allow them to access records for which they are the OPR or Backup OPR.
  - **User-IPT**: allows the user to only view CCaR records assigned to their IPT. The user can create new CCaR records and edit existing CCaR records where they are assigned as the OPR or Back-up OPR. The user is prevented from accessing many reports and tools. Reports and tools accessible to the user will only allow them to access records for their IPT
  - **User-Full:** allows the user to view all CCaR records. The user can create new CCaR records and edit existing CCaR records where they are assigned as the OPR or Back-up OPR. If the "Allow Users with Budget Docs-Full Priv to Edit CCaR Records Referencing That Budget" option is checked under System Settings / CCaR Options and if the user has Budget "DOCS" privileges "FULL" on any budget assigned to a CCAR record, the user will also be able to edit the Working copy of any CCaR record containing that budget as well as the ability to add and delete attachments.
  - **IPT-CHIEF**: in addition to User-Full privileges, the user has the ability to edit all CCaR records within their assigned IPT and the ability to reassign CCaR OPRs and IPTs.
  - **Supervisor:** allows the user the ability to edit all CCaR records and access to the Admin menu.
- **Contract Module Privileges**
  - **None:** prevents the user from accessing the Contract Management menu.
  - **Read-Only:** allows read-only access in the Contract Management menu.
  - **User-Restricted:** user may only view contracts they have been assigned as a contract user. Only contracts the user has been assigned to as a contract user will be visible in the Contract List.
  - **User:** allows the user to add new contracts and add, edit and delete contract modifications and vouchers for contracts where they are assigned as a user. Allows read-only access to all other contracts.
  - **User-Full:** allows the user full access to the Contract Management menu. The user can add new contracts and add, edit and delete contract modifications and vouchers.
  - **Supervisor:** in addition to User-Full privileges, the user can delete contracts from the

Contract List and load and import data under Interface Status.

- **Recon Module Privileges**
  - **None:** prevents the user from accessing the Reconciliation menu.
  - **Read-Only:** allows the user read-only access in the Reconciliation menu.
  - **Travel:** allows the user access to reconcile Travel Recon data but will have read-only privileges for COE Recon.
  - **User-Bud:** allows the user to reconcile data in Travel and COE for budgets where the RECON box is checked under User / Budget Privileges.
  - **User-Full:** in addition to User-Bud privileges, allows the user to access DFAS Interface Configuration Tool. The user can process the DFAS-CCaR Data Link and DFAS-CCaR Travel Link under Data Transfer, process DFAS backfills and view criteria. The user can link, un-link, backfill and edit allocations on all documents.
  - **Supervisor:** in addition to User-Full privileges, the user to process the DFAS Data Transfer and DFAS Travel Transfer in the DFAS Interface Configuration Tool. The data under View Criteria may be edited if the CCaR Database Administrator (DBA) assigns the appropriate grant for the user.
- **Incoming Document Tool Privileges**
  - **None:** prevents the user from accessing Incoming Documents. If the user has access to CCaR records, funded by an Incoming Document budget, the user can view CCaR record forecasts and execution data.
  - **Read-Only:** allows the user read-only access to Incoming Documents.
  - **User-Exec:** same as the Read-Only privilege, plus, allows the user to create funding documents and forecasts for Incoming Document Budgets.
  - **User-Full:** in addition to User-Exec privileges, allows the user to add, edit and delete Incoming Documents.
- **Recon Issues Module Privileges**
  - **None:** prevents the user from accessing Recon Issues.
  - **Read-Only:** allows the user read-only access to Recon Issues.
  - **User-Full**: allows the user to create and edit Recon Issues where they are assigned as the OPR. The user may not delete any Recon Issues.
  - **Supervisor:** in addition to User-Full privileges, allows the user the ability to edit and delete all Recon Issues and import issues into the system.
- **Target Load Module Privileges**
  - **None:** prevents the user from accessing the Target Load Tool.
  - **User-Limited:** allows the user access to the Target Load Tool. The user can create Target Load Sheets (TLSs), edit their own TLSs, but cannot increase or decrease the overall amount of a budget. The user may only change amounts on addresses on a TLS that equal a zero-sum gain.
  - **User:** allows the user access to the Target Load Tool. The user can create and edit their TLSs.
  - **User-ALO:** same as the User privilege, plus, the user has the ability to mark TLSs as processed in GAFS and create WINGAMPS import files. For installation TLSs, the user can see approved, in-process and rejected data from linked organizations, in addition to

their own, if the user has a CCaR account in the linked organization(s). This applies to TLSs, WINGAMPS and GAFS Address Requests.

- **Multi-Org Privileges**
  - **User-Org:** when selected, the user may only view data in Multi-Org reports and tools for the organization(s) assigned to their account. The user may only login to the organization(s) assigned to their account. This is the default privilege assigned.
  - **User-Full:** when selected, the user may view data in Multi-Org reports and tools for all organizations. The user may only login to the organization(s) assigned to their account.
  - **Supervisor:** when selected, the user may view data in Multi-Org reports and tools for all organizations. The user may login to all organizations. The user may access the Admin menu in all organizations and access Multi-Org Admin System Settings.

Executive CCaR

Executive CCaR is also part of the PMRT suite of tools. It is a read only dashboard that provides financial and programmatic data to decision makers. There are only two roles defined within Executive CCaR. Details on those roles is shown below:

- **User:** The user role in Executive CCaR allows users the ability to access Executive CCaR. Visibility of what they can see in the dashboard is defined by what level of the Executive CCaR taxonomy they have access to. For example the PEO for Tankers is given user access to only the Tanker portion of the hierarchy. He or she can see everything within the Tanker PEO, but would not have visibility to any of the other PEOs.
- **Administrator**: The Administrator role in Executive CCaR allows the user to create, update and delete accounts. They also have the ability to assign what level of the taxonomy a user account has access to.

Data Access Program Reporting (DAPR)

DAPR is also part of the PMRT suite of tools. It is an application that is utilized by SAF/AQ and AFLCMC to manage the Acquisition Master List(AML), the Investment Master List(IML), and the Workload Master List (WML). Details on the roles that are available within DAPR are shown below:

- **Read Only –** Users granted this role can view all of the information in the tool, but cannot make any changes to it.
- **DAPR IML ANALYST -** Users granted this role may be selected as a Lead Analyst on an IML program.
- **DAPR IML EDIT ALL** - Users granted this role will have the ability to modify, approve, disapprove and archive any IML program.
- **DAPR IML EDIT ORG** - Users granted this role will have the ability to modify, approve, disapprove and archive IML program within their assigned organization(s).
- **DAPR NON-IML ANALYST** - Users granted this role may be selected as a Lead Analyst on a Non-IML program.
- **DAPR NON-IML EDIT ALL** - Users granted this role will have the ability to modify, approve, disapprove and archive any Non-IML program.
- **DAPR NON-IML EDIT ORG** - Users granted this role will have the ability to modify, approve, disapprove and archive any Non-IML program within their assigned organization(s).

Enterprise Reports

The PMRT Enterprise reports is also part of the PMRT suite of tools. It is an Ad-Hoc reporting capability that allows users to generate report based off of pre-defined templates. Details on the roles that are available within Enterprise Reports are shown below:

- **User** - Users granted this role are allowed to generate reports and save them to their own personal folder

Resource Identification Tool (RIT)

The Resource Identification Tool (RIT) is also part of the PMRT suite of tools. It is utilized by AFLCMC to approve new work packages submitted by the field. Details on the roles that are available within the Resource Identification Tool is shown below:

- **Read Only –** Users granted this role can view all of the information in the tool, but cannot make any changes to it.
- **Division Approver** - Users granted this role are responsible for approving incoming new work packages at the division/Program Office level prior to the Directorate level approver.
- **Directorate Reviewer** - Users granted this role are responsible for the initial review of the new work package to determine if the work is valid for the Directorate.
- **Directorate OSF-PM** - Users granted this role are the designated Program Management (PM) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required PM resources are correctly identified.
- **Directorate OSF-FM** - Users granted this role are the designated Financial Management (FM) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required FM resources are correctly identified.
- **Directorate OSF-EN** - Users granted this role are the designated Engineering (EN) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required EN resources are correctly identified.
- **Directorate OSF-PK** - Users granted this role are the designated Contracting (PK) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required PK resources are correctly identified.
- **Directorate OSF-LG** - Users granted this role are the designated Logistics (LG) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required LG resources are correctly identified.
- **Directorate OSF-TE** - Users granted this role are the designated Test & Evaluation (TE) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required TE resources are correctly identified.
- **Directorate OSF-COS** - Users granted this role are the designated Cyberspace Operation Support (COS) Organization Senior Functional(OSF) within their directorate and have the
- responsibility for review of the new work package to insure that the required COS resources are correctly identified.
- **Directorate OSF-IN** - Users granted this role are the designated Intelligence (IN) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required IN resources are correctly identified.

- **Directorate OSF-NFA** - Users granted this role are the designated Non Functionally Aligned (NFA) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required NFA resources are correctly identified.
- **Directorate OSF-IP** - Users granted this role are the designated Information Protection (IP) Organization Senior Functional(OSF) within their directorate and have the responsibility for review of the new work package to insure that the required IP resources are correctly identified.
- **Directorate Facilities Manager** - Users granted this role are responsible to identify preliminary facilities required for new work based on Directorate resources.
- **Directorate Resources Analyst** -Users granted this role are responsible for reviewing all new work packages to insure that all inputs are accurate.
- **Directorate Approver** - Users granted this role are responsible for the approval of all new work packages submitted from their Directorate
- **XPO Reviewer** - Users granted this role are responsible for insuring that the new work package contains all of the required information before it continues through the new workload approval process
- **DP Manpower Reviewer** - Users granted this role are responsible for insuring that all requested resources identified on the new work packages are accurate and sufficient to support the new work being requested
- **Directorate CSF-PM** - Users granted this role are the designated Program Management (PM) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required PM resources are correctly identified.
- **Directorate CSF-FM** - Users granted this role are the designated Financial Management (FM) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required FM resources are correctly identified.
- **Directorate CSF-EN** - Users granted this role are the designated Engineering (EN) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required EN resources are correctly identified.
- **Directorate CSF-PK** - Users granted this role are the designated Contracting (PK) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required PK resources are correctly identified.
- **Directorate CSF-LG** - Users granted this role are the designated Logistics (LG) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required LG resources are correctly identified.
- **Directorate CSF-TE** - Users granted this role are the designated Test & Evaluation (TE) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required TE resources are correctly identified.
- **Directorate CSF-COS -** Users granted this role are the designated Cyberspace Operation Support (COS) Center Senior Functional(CSF) within their directorate and have the

responsibility for review of the new work package to insure that the required COS resources are correctly identified.

- **Directorate CSF-IN -** Users granted this role are the designated Intelligence (IN) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required IN resources are correctly identified.
- **Directorate CSF-NFA** - Users granted this role are the designated Non Functionally Aligned (NFA) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required NFA resources are correctly identified.
- **Directorate CSF-IP** - Users granted this role are the designated Information Protection (IP) Center Senior Functional(CSF) within their directorate and have the responsibility for review of the new work package to insure that the required IP resources are correctly identified.